

REMARKS

Claims 1-15 have been pending.

Claim 11 is rejected under 35 USC 112, second paragraph, for indefiniteness. Claim 11 is amended, taking into consideration the Examiner's comments. Withdrawal of the indefiniteness rejection of claim 11 is respectfully requested.

Claims 1, 4, 9, 14 and 15 are rejected under 35 USC 102(b) as being anticipated by Bruce Schneier "Applied Cryptography."

Claims 2 and 6-8 are rejected under 35 USC 103(a) as being unpatentable over Schneier in view of Barrett (US Patent No. 5,222,137).

Claims 3 and 5 are rejected under 35 USC 103(a) as being unpatentable over Schneier.

Claims 10 and 11 are rejected under 35 USC 103(a) as being unpatentable over Schneier in view of Colvin (US Patent No. 6,041,123).

Claims 12 and 13 are rejected under 35 USC 103(a) as being unpatentable over Schneier in view of "Mapping a Network Drive."

Claims 1, 2, 3, 6, 9, 10, 11, and 13-15 are amended, claims 4, 5, 7, 8, and 12 are cancelled without disclaimer or prejudice, and new claim 16 is added. Thus, claims 1-6, 9-11, and 13-16 are pending for reconsideration, which is respectfully requested.

No new matter is in this Amendment. The foregoing rejections are hereby traversed.

SPECIFICATION

The specification is amended to correct an error in view of FIG. 2.

DRAWINGS

According to the foregoing, FIGS. 7 and 16 are amended to correct errors in operations 34 and 108, respectively. Support for the drawing amendments can be found, for example, in page 17, lines 10-15 and page 20, lines 8-14, of the present Application. Entry of the drawing replacement sheets for FIGS. 7 and 16 (two replacement drawing sheets) is respectfully requested.

PRIOR ART REJECTIONS

INDEPENDENT CLAIMS 1, 9, 14 and 15

Claims 1, 4, 9, 14 and 15 are rejected under 35 USC 102(b) as being anticipated by Bruce Schneier "Applied Cryptography."

The Examiner relies on Schneier, page 217, FIG. 10.1, description of link-by-link encryption at the physical layer, in which each node at the physical layer decrypts (e.g., node 2, Dk1, for decryption) and encrypts (e.g., node 2, Ek2, for encryption). Therefore, the Examiner is alleging that in Schneier, node 2, Dk1 and Ek2, is similar to the claimed present invention's "individual key" and "communication key."

However, in contrast to the link-by-link encryption described in Schneier, the claimed present invention provides using **both "an individual key" and "a communication key"** at a **"transmission side,"** where the **"individual key"** is used, upon transmission in the transmission side, for decoding data that is enciphered with the **"individual key,"** and the **decoded data is then enciphered with the "communication key" for the transmission.** See, FIG. 4, operations 21 and 22 at the transmitting side, of the present Application.

Accordingly, in contrast to Schneier, independent claims 1, 3 (drawn to a reception side processing), 14 and 15, using claim 1 as an example, are amended to clarify the patentably distinguishing features of the present invention, as follows.

1. (CURRENTLY AMENDED) A cryptographic communication method, ~~comprising: in which a communication key is used for enciphering data to be transmitted in the transmission side, and a key is used for decoding received data in the reception side, wherein in the transmission side~~

individually authenticating, in a transmission side, a communication key and an individual key that is different from the communication key, thereby using both keys ~~is used for enciphering the data to be transmitted,~~

determining, in the transmission side, **whether a target file is enciphered by the individual key.**

decoding the target file using the individual key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered; and

enciphering for transmission, in the transmission side, the decoded target file or the unprocessed target file that is not enciphered, **using the communication key,** ~~the enciphered data are decoded by using the individual key first, and then the decoded data are enciphered by using the communication key so that the enciphered file can be transmitted~~

wherein in the transmission side, the decoding and the enciphering using the communication key are performed continuously, if the decoding is performed (emphasis added).

Further, dependent claim 13 (drawn to a file access system) is rewritten into independent form, canceling independent claim 12, and also amended along the lines of amended claim 1.

Support for the claim amendments can be found, for example, in page 9, line 4 to page 13, line 5, and FIGS. 2, 3, 4, 7 and 8, of the present Application.

Further, independent claim 9, (drawn to a file access system, including “an enciphered folder” and transmission side processing), 10 (drawn to a file access system and transmission side processing) and 11 (drawn to a file access system and reception side processing) are amended to clarify the patentably distinguishing features of the present invention. For example, in contrast to Schneier, amended independent claim 9 provides:

9. (CURRENTLY AMENDED) A file access system, wherein two different keys are authenticated individually ~~so that they can be used~~, and for data transmission, a decoding process decodes enciphered data stored in an enciphered folder using one of the keys, and an enciphering process automatically enciphers the decoded data for the transmission using the other of the keys ~~are performed continuously for one file~~.

INDEPENDENT CLAIM 6

Claims 2 and 6-8 are rejected under 35 USC 103(a) as being unpatentable over Schneier in view of Barrett (US Patent No. 5,222,137). In contrast to Schneier and Barrett, independent claim 6 is amended along the lines of amended independent claim 1 and by incorporating the patentably distinguishing features of dependent claims 7 and 8. Dependent claims 7 and 8 are cancelled without disclaimer or prejudice.

NEW INDEPENDENT CLAIM 16

In contrast to the link-by-link encryption described in Schneier, the claimed present invention as recited in new independent claim 16 provides using **both “an individual key” and “a communication key”** at a **“transmission side,”** where the **“individual key”** is used, upon transmission in the transmission side, for decoding **“enciphered data stored in an enciphered folder at the transmission side,”** and the **decoded data is then enciphered with the “communication key” for the transmission.** See, FIG. 4, operations 21 and 22, and enciphered folder (FA) and unencrypted folder (FH), at the transmitting side, of the present Application.

16. (NEW) A cryptographic communication method, comprising:

using **a communication key for enciphering data to be transmitted** by a transmission side, and

using **an individual key for decoding enciphered data** stored in **an enciphered folder** at the transmission side,

wherein in the transmission side, **the individual key is different from the communication key** used for enciphering the data to be transmitted, **first, the stored enciphered data are decoded using the individual key, and, second, the decoded data is enciphered using the communication key for transmission.**

Schneier does not disclose or suggest the claimed present invention's “in the transmission side, the **individual key is different from the communication key** used for enciphering the data to be transmitted, **first, the stored enciphered data are decoded using the individual key, and, second, the decoded data is enciphered using the communication key for transmission.**”

Support for the new claim 16 can be found, for example, in FIG. 4 and page 11, line 29 to page 12, line 19, of the present Application.

CONCLUSION


In view of the claim amendments and the remarks, withdrawal of the rejection of pending claims and allowance of pending claims is respectfully requested.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: October 8, 2004

By: 
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501